tbr THE COLLEGE SYSTEM of TENNESSEE

TENNESSEE BOARD OF REGENTS
Special Called Meeting of the Board
Tuesday, May 14, 2019 - 4:00 PM (CDT)

I. Call the Meeting to Order

II. Call the Roll

III. Review and Consider Building Naming Request from Pellissippi State Community College *(Chancellor Tydings)*

IV. Review and Consider Proposed Revisions to TBR Policies

a. Policy 1:08:04:00 Personally Identifiable Information *(Gibbs)*
b. Policy 1:08:03:00 Access Control *(Gibbs)*
c. Policy 1:08:01:00 Enterprise Information Systems Updates *(Gibbs)*
d. Policy 1:08:05:00 IT Acceptable Uses *(Gibbs)*
e. Policy 2:01:00:04 Awarding of Credits Earned through Extra-Institutional Learning to Community Colleges and Universities *(Schulte)*
f. Policy 2:02:00:01 Reserve Officer Training Corps Programs *(Schulte)*
g. Dissolution of Policy 5:02:05:00 Employment of Graduate Assistants *(Schulte)*

V. Adjourn

tbr THE COLLEGE SYSTEM
of TENNESSEE

BOARD TRANSMITTAL

MEETING:	Special Called Board Meeting
SUBJECT:	Building Naming Request from Pellissippi State Community College
DATE:	May 14, 2019
PRESENTER:	Flora W. Tydings
PRESENTATION REQUIREMENT:	5 minutes with discussion
ACTION REQUIRED:	ROLL CALL VOTE
STAFF'S RECOMMENDATION:	Approve

The Board will review and consider a building naming request submitted by Pellissippi State Community College for the new math and science building at the Hardin Valley campus.

The naming committee was comprised of Judy Sichler, president of Faculty Senate, Kane Barker, dean of Natural and Behavioral Sciences, Nancy Pevey, dean of Mathematics, Aneisa Rolen, executive director of the Pellissippi State Foundation, Mandy Hogan, student representative, and ex-officio member President Anthony Wise.

At that meeting President Wise reviewed TBR's policy on building namings and discussed the academic programs to be housed at this new facility. In addition, he discussed the capital fundraising campaign in support of the cost of the building, and possible naming opportunities.

This request is in compliance with TBR Policy 4:02:05:01 - Naming Buildings and Facilities and Building Plaques.

tbr THE COLLEGE SYSTEM of TENNESSEE

BOARD TRANSMITTAL

MEETING:	Special Called Board Meeting
SUBJECT:	Personally Identifiable Information (PII) 1:08:04:00
DATE:	May 14, 2019
PRESENTER:	Danny Gibbs
PRESENTATION REQUIREMENTS:	
ACTION REQUIRED:	Roll Call Vote
STAFF'S RECOMMENDATION:	Approval

BACKGROUND INFORMATION:

This policy contains changes that are minor in nature and include the modernization of language used by IT professionals and minor corrections relating to laws and practices across the system.

This policy has been reviewed and approved by CIOs at the various institutions, by the Business Affairs Sub-Council and the Presidents.

Attachment(s): Personally Identifiable Information (PII) 1:08:04:00

Personally Identifiable Information (PII) 1:08:04:00

Policy Area

General Policy

Applicable Divisions

TCATs, Community Colleges, System Office, Board Members

Purpose

TBR institutions create, collect, maintain, use, and transmit personally identifiable information relating to individuals associated with the institution including, but not limited to, students, alumni, faculty, administrators, staff, and service employees. ~~The institution is~~TBR institutions are committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations in order to maximize trust and integrity.

Definitions

- Data Custodians: Data Custodians are the people responsible for oversight of personally-identifiable information in their respective areas of institutional operations. ~~The Data Custodian is a person who has technical control over an information asset or dataset, for example system administrators, DBAs, CIOs, etc.~~
- The Data Owner (also called a Data Steward) is the person who has administrative control and has been officially designated as accountable for a specific information asset or dataset. This person would determine who has access to what and IT implements the controls to match.
- Minimum Necessary: Minimum Necessary is the standard that defines that the least information and fewest people should be involved to satisfactorily perform a particular function.
- Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their ~~name,~~ ID, Social Security

number, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

- Directory information: Directory information is information that is generally not considered harmful or an invasion of privacy if released. It can also be disclosed to outside organizations. ~~Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks.~~

Commented [TA1]: I don't think this is needed, and the specific examples are not very relevant.

Policy

I. Policy

A. Members of the TBR community shall employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all personally identifiable information (PII), irrespective of its source or ownership or the medium used to store it.

B. All individuals who dispense, receive, and store PII have responsibilities to safeguard it.

C. In adopting this policy, the System is guided by the following objectives:

1. To enhance individual privacy for members of the TBR community through the secure handling of PII.~~ and personal identifiers (PIDs);~~
2. To ensure that all members of the TBR community understand their obligations and individual responsibilities under this policy by providing appropriate training that shall permit the TBR community to comply with both the letter and the spirit of all applicable privacy legislation. Each member institution will be responsible for determining the means of training for its institution.~~;~~
3. To increase security and management of Social Security numbers (SSNs) by:

a. Instilling broad awareness of the confidential nature of the SSNs;

b. Establishing a consistent policy about the use of SSNs throughout the System; and

c. Ensuring that access to SSNs for the purpose of conducting TBR business is granted only to the extent necessary to accomplish a given task or purpose.

d. To reduce reliance on the SSN for identification purposes as much as possible.

4. To comply with all Payment Card Industry (PCI) standards

~~5. To comply with HIPPA standards (if applicable)~~

~~6.~~5. To comply with any other applicable and required standards, regulations and/or laws

~~7.~~6. To comply with Family Educational Rights and Privacy Act of 1974 (FERPA)~~FERPA standards~~

D. Data Custodians are responsible for oversight of personally identifiable information in their respective areas of institutional operations. Activities of these officials are aligned and integrated through appropriate coordination among these cognizant institutional officials.

II. Scope

A. This policy applies to all members of the TBR community, including all full- and part-time employees, faculty, students and their parents or guardians, and other individuals such as volunteers, contractors, consultants, other agents of the community, alumni, and affiliates that are associated with the System or whose work gives them custodial responsibilities for PII.

III. Policy Requirements

A. Data Trustees

1. Officials responsible for each of the following areas shall be considered data custodians:

a. Student Records

~~a.~~b. Financial Aid Records

~~b.~~c. Alumni and Donor Records

~~c.~~ E~~Health Records~~

d. ~~Faculty and Staff~~Employee Records

e. Purchasing and Contracts

f. Research Subjects

g. Public Safety or Campus Police

IV. Personally Identifiable Information

A. PII may be released only on a Minimum Necessary basis and only to those individuals who are authorized to use such information as part of their official TBR duties, subject to the requirements:

1. That the PII released is narrowly tailored to a specific business requirement;
2. That the information is kept secure and used only for the specific official TBR [business] purposes for which authorization was obtained; and
3. That the PII is not further disclosed or provided to others without proper authorization as defined above.

B. PII may be handled by third parties, including cloud service providers, with the strict requirement that the information be kept secure and used only for a specific official authorized business purpose as defined in a Business Associate Agreement with that third party.

C. Exceptions to this policy may be made only upon specific requests approved by the cognizant institutional official responsible for such information as specified in this policy and only to the degree necessary to achieve the mission and business needs of the institution.

1. Exceptions made must be documented, retained securely, and reviewed periodically by the appropriate cognizant institutional official or his/her designee.

2. Exceptions may be modified or eliminated based on this review and shall be documented and retained for auditing purposes.

D. Directory Information, as defined by Federal and State law and institutional policy, will be published following the guidelines defined by the ~~institution~~specific law.

E. Based on FERPA guidelines, directory information is information that is generally not considered harmful or an invasion of privacy if released and can be disclosed without consent.

F. Schools must notify students annually of their rights under FERPA.~~ to not disclose directory information~~

Commented [TA2]: I removed this to reduce the risk of confusion. We are required to notifiy students annually of all their rights under FERPA, not just directory op-out.

G. Information that has been collected that conforms to the HIPAA standards of de-identification or anonymization is not PII.

V. Government-Issued Personal Identifiers

A. Social Security Number

1. Provision of Information

a. TBR institutions collect SSNs:

1. When required to do so by law;

2. When no other identifier serves the business purpose; and

3. When an individual volunteers the SSN as a means of locating or confirming personal records.

b. In other circumstances, individuals are not required to provide their SSN verbally or in writing at any point of service, nor are they to be denied access to those services should they refuse to provide an SSN.

2. Release of SSNs

a. SSNs will be released to persons or entities outside the institution only:

1. As required by law;

2. When permission is granted by the individual;

3. When the external entity is acting as the institution’s authorized contractor or agent and attests that no other methods of identification are available, and reasonable security measures are in place to prevent unauthorized dissemination of SSNs to third parties; or

4. When the appropriate Counsel has approved the release.

3. Use, Display, Storage, Retention, and Disposal

a. SSNs or any portion thereof will not be used to identify individuals except as required by law or with approval by a cognizant TBR official for a TBR business purpose.

b. The release or posting of personal information, such as grades or occupational listings, keyed by the SSN or any portion thereof, is prohibited, as is placement of the SSN in files with unrestricted access.

c. SSNs will be transmitted electronically only for business purposes approved by the institutional officials responsible for SSN oversight and only through secure mechanisms.

d. The Data Custodians who are responsible for SSNs will oversee the establishment of business rules for the use, display, storage, retention, and disposal of any document, item, file, or database which contains SSNs in print or electronic form.

B. Non-SSN Government-Issued Identifiers

1. In the course of its business operations, TBR institutions have access to, collect, and use non-SSN government-issued identifiers such as driver's licenses, passports, HIPAA National Provider Identifiers, Employee Identification Numbers (EIN), and military identification cards, among others.

2. TBR institutions shall follow the Minimum Necessary standard and strive to safeguard these identifiers.

VI. TBR Institution-Issued Identifiers

A. Institutional ID Number

1. Assignment Eligibility and Issuance

    a. The institutional id is a unique alphanumeric identifier assigned by the institution to any entity that requires an identifying number in an institutional system or record.

    ~~a.~~b. An Institutional ID is assigned at the earliest possible point of contact between the entity and the institution.

    ~~b.~~c. The Institutional ID is associated permanently and uniquely with the entity to which it is assigned.

2. Use, Display, Storage, Retention, and Disposal

    a. The Institutional ID is considered PII by the institution, to be used only for appropriate business purposes in support of operations.

    b. The Institutional ID is used to identify, track, and serve individuals across all institutional electronic and paper data systems, applications, and business processes throughout the span of an individual's association with the institution and presence in the institution's systems or records.

    c. The Institutional ID is not to be disclosed or displayed publicly by the Institution, nor to be posted on the institution’s electronic information or data systems unless the Institutional ID is protected by access controls that limit access to properly authorized individuals.

    d. The release or posting of personal information keyed by the Institutional ID, such as grades, is prohibited.

    e. Any document, item, file, or database that contains Institutional IDs in print or electronic form is to be protected and disposed of in a secure manner in compliance with data retention rules.

VII. Other Externally-Assigned Identifiers and Other Personally Identifiable Information

A. TBR institutions shall follow the Minimum Necessary standard and strive to safeguard any externally assigned identifiers which may be collected.

VIII. Responsibility for Maintenance and Access Control

A. Institutional IDs are maintained and administered by the appropriate institutional office in accordance with this policy.

1. Other institutional offices may maintain and administer electronic and physical repositories containing personal identification numbers for uses in accordance with this policy.

B. Access to electronic and physical repositories containing PII ~~will~~ shall be controlled based upon reasonable and appropriate administrative, physical, technical, and organizational safeguards.

Formatted: Font: Not Bold

Formatted: Font: Not Bold, No underline

C. Individuals who inadvertently gain access to a file or database containing PII should report it to the appropriate authority.

~~D. Disk-level encryption for employee computers shall be part of the daily workflow.~~

~~E.~~D. All paper documents with PII must be under lock and key or otherwise securely stored.

~~F.~~E. Document retention policies dictate schedules for PII deletion and/or destruction. Proper disposal of PII shall involve cross-cut shredders (for paper), securely wiping/deleting data (for digital information) and other information security approved methods of eliminating this data.

IX. Enforcement

A. Violations of this policy resulting in misuse of, unauthorized access to, or unauthorized disclosure or distribution of personal identification numbers may subject individuals to legal and/or disciplinary action, up to and including the termination of employment or contract with the Institution or, in the case of students, suspension or expulsion from the institution.

Sources

NEW Guideline approved at August 19, 2014 President's Meeting; effective September 26, 2014.

Related Policies

- Information Technology Resources

THE COLLEGE SYSTEM of TENNESSEE

BOARD TRANSMITTAL

MEETING:	Special Called Board Meeting
SUBJECT:	Access Control: 1:08:03:00
DATE:	May 14, 2019
PRESENTER:	Danny Gibbs
PRESENTATION REQUIREMENTS:	
ACTION REQUIRED:	Roll Call Vote
STAFF'S RECOMMENDATION:	Approval

BACKGROUND INFORMATION:

This was a guideline that we recommend become a policy. The purpose of this policy is to establish a minimum expectation with respect to access controls in order to protect data stored on computer systems throughout the system. Updates have been made to be inclusive of all TBR Institutions. Additionally, procedures were added to the policy to ensure that all institutions are following the same protocols regarding password construction and password management,

This policy has been reviewed and approved by CIOs at the various institutions, by the Business Affairs Sub-Council, and by the Presidents.

Attachment(s): Access Control Policy 1:08:03:00

Access Control: ~~G-052~~1:08:03:00

~~Guideline~~Policy Area

General ~~Guidelines~~Policies

Applicable Divisions

TCATs, Community Colleges, ~~Universities,~~ System Office, Board Members

Purpose

The purpose of this ~~guideline~~policy is to establish a minimum expectation with respect to access controls in order to protect data stored on computer systems throughout the system.

~~Guideline~~Policy

I. Policy

A. Tennessee Board of Regents institutions shall control user access to information assets based on requirements of individual accountability, need to know, and least privilege.

B. Access to institutional information assets must be authorized and managed securely in compliance with appropriate industry practice and with numerous applicable legal and regulatory requirements (e.g., the Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, the Open Records Act of Tennessee, Gramm Leach Bliley Act, and identity theft laws).

C. Institutional information assets include data, hardware and software technologies, and the infrastructure used to process, transmit, and store information.

1. Any computer, laptop, printer or device that an authorized user connects to the campus network is subject to this policy.

Formatted: Strikethrough

Formatted: No underline

Formatted: Strikethrough

Formatted: No underline

Formatted: Strikethrough

Formatted: Font: Not Bold, No underline

Formatted: Strikethrough

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, Strikethrough

Formatted: No underline

Formatted: Font: Not Bold, Not Strikethrough

2. Guest, unauthenticated access may be provisioned commensurate with usage and risk.

3. Authorized users accessing institutional computing resources and network with their own personal equipment are responsible for ensuring the security and integrity of the systems they are using to establish access.

~~3.~~4. For systems that contain critical or confidential classified data, TBR and its institutions shall use secure methods that uniquely identify and authenticate users. Such methods can include multi-factor authentication, passwords, data loss prevention, device management, biometrics and public/private key pairs.

~~TBR Office of Information Technology shall deploy a combination of multi-factor authentication, data loss prevention and device management for any accounts/devices connecting to systems containing critical or extremely confidential classified data.~~

Formatted: Font: Not Bold, No underline

~~The multi-factor authentication tool that will be deployed is the Microsoft Multifactor Authentication resident in Microsoft Azure. Rollout of this application will follow a phased-in approach, offering opt-in self service initially and then a comprehensively planned implementation for all faculty and staff.~~

Formatted: Font: Not Bold, No underline

~~4. A significant training and communication plan will be introduced explaining the benefits and safeguards inherent in multi-factor authentication.~~

II. Access Controls

A. Access to information assets must be restricted to authorized users and must be protected by appropriate physical, administrative, and logical authentication and authorization controls.

B. Protection for information assets must be commensurate with the classification level assigned to the information.

C. Each computer system shall have an automated access control process that identifies and authenticates users and then permits access based on defined requirements or permissions for the user or user type.

D. All users of secure systems must be accurately identified, a positive identification must be maintained throughout the login session, and actions must be linked to specific users.

E. Access control mechanisms may include user IDs, access control lists, constrained user interfaces, encryption, port protection devices, secure gateways/firewalls, and host-based authentication.

III. User Identification, Authentication, and Accountability

A. User IDs:

1. The access control process must identify each user through a unique user identifier (user ID) account.
2. User IDs are assigned by the campus ~~(~~or ~~system~~TBR~~)~~ O~~o~~ffice of I~~i~~nformation T~~t~~echnology and application support personnel.
3. Users must provide government-issued, picture IDs for positive proof of identity when receiving account access.
4. Users must provide their user ID at logon to a computer system, application, or network.

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

B. Individual Accountability:

1. Individual accountability must be maintained.
2. ~~**Each and e**every~~Each user ID must be associated with an individual person who is responsible for its use.
3. Individuals with authenticated access cannot share their login credentials with anyone with the penalty of having their access rescinded immediately.

Formatted: Font: Not Bold, No underline

C. Authentication:

1. Authentication is the means of ensuring the validity of the user identification.
2. All user access must be authenticated.

a. The minimum means of authentication is a personal secret password that the user must provide with each system and/or application logon.

b. All passwords used to access information assets must conform to certain requirements relating to password composition, length, expiration, and confidentiality. Please refer to 1:08:02:00~~G-051~~, ~~Password Management~~Digital Identity and Authentication Management for additional requirements.

Formatted: Font: (Default) Arial, 12 pt, Font color: Custom Color(RGB(52,64,81))

~~c. Granting access to the central multi-entity processing (MEP) single instance of the ERP system includes authentication through multi-factor authentication controls to enable security layering.~~

Formatted: Font: Not Bold, No underline

IV. Access Privileges

A. Each user's access privileges shall be authorized on a need-to-know basis as dictated by the user's specific and authorized role.

B. Authorized access ~~will~~ shall be based on least privilege.

Formatted: Font: Not Bold

Formatted: Font: Not Bold, No underline

1. This means that only the minimum privileges required to fulfill the user's role shall be permitted.

Formatted: Not Strikethrough

2. Access privileges shall be ~~must be~~ defined to ~~so as to~~ maintain appropriate segregation of duties to reduce the risk of misuse of information assets.

3. Any access that is granted to data must be authorized by the appropriate data trustee.

C. Access privileges shall ~~should shall~~ be controlled based on the following criteria, as appropriate:

1. Identity (user ID);
2. Role or function;
3. Physical or logical locations;
4. Time of day/week/month;
5. Transaction based access;
6. Access modes such as read, write, execute, delete, create, and/or search.

D. Privileged access (e.g., administrative accounts, root accounts) must be granted based strictly on role requirements.

   1. The number of personnel with special privileges should be carefully limited.

V. Access Account Management

A. User ID accounts must be established, managed, and terminated to maintain the necessary level of data protection.

B. The following requirements apply to network logons as well as individual application and system logons, and should be implemented where technically and procedurally feasible:

   1. Account creation requests must specify access either explicitly or ~~to~~ request a role that has been mapped to the required access.

      a. New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights.

   2. Accounts must be locked out ~~after five~~ according to individual campus requirements after an institution-defined number of consecutive invalid logon attempts.

      a. When a user account is locked out, it should remain locked out for a minimum of five minutes or until authorized personnel unlocks the account.

   3. User interfaces must be locked ~~after no more than twenty minutes five~~ according to individual campus requirements after an institution-defined length of system/session idle time.

      a. This requirement applies to workstation and laptop sessions as well as application sessions where feasible.

      b. The office of information technology shall implement measures to enforce this requirement and to require the user to re-authenticate to reestablish the session.

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold, No underline

Formatted: Not Strikethrough

4. Systems housing or using restricted information must be configured in such a way that access to the restricted information is denied unless specific access is granted.

   a. Access to restricted information is never to be allowed by default.

5. ~~Access must be~~ Information Technology personnel revoke~~d immediately~~ access upon notification that access is no longer required in accordance with the following procedures.

   a. Access privileges of terminated or transferred users must be revoked or changed as soon as ~~possible~~ notification of termination or transfer occurs and in accordance with stakeholders of contract control at the local institutions.

   b. In cases where an employee is not leaving on good terms, the user ID must be disabled simultaneously with departure.

   c. Access for users who are on leaves of absence or extended disability must be suspended until the user returns.

   d. Adjunct faculty members are never granted access to Banner ~~INB accounts~~Admin Pages.

   e. Adjunct faculty member account access shall be controlled by a procedure resident at the local institutions using contract status, defined dates of employment and information from other stakeholders with contract control for adjunct faculty.

   f. Using the above-mentioned procedure, each campus will run this process on a campus-defined schedule according to academic calendars ~~calendars (i.e. the second week of the next semester)~~ and direction from stakeholders with contract control for adjunct faculty. This process shall be determined by individual campuses.

   g. Adjunct faculty members shall be granted limited access before and after their course start and end dates ~~(~~to perform the duties necessary for their

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

position~~)~~, upon request ~~(~~involving reasons for the extension and specific access~~)~~.

6. User IDs will be disabled after a period of inactivity that is determined appropriate by the current business process and the individual campus.
7. All third party access (contractors, business partners, consultants, vendors) must be authorized and monitored using processes determined by the individual campuses.
8. Appropriate logging will be implemented commensurate with sensitivity/criticality of the data and resources.
   a. Logging of attempted access must include failed logons.
   b. Where practical, successful logons to systems with restricted information shall be logged.
   c. Logs should be monitored and regularly reviewed to identify security breaches or unauthorized activity.
   d. Logs ~~should~~ shall be maintained for at least ninety days.
9. A periodic audit of secured systems to confirm that access privileges are appropriate must be conducted.
   a. The audit will consist of reviewing and validating that user access rights are still needed and are appropriate.
   ~~b. Timeliness of the audit shall be commensurate with the classification of data access granted to each account.~~
10. Applications requiring an account not tied to a single user shall employ service-based accounts
   a. Users oversee these accounts and maintain their passwords.
   b. Applications requiring these accounts shall be monitored and audited by individual campus documented procedures dictated by the application for which they are provisioned.

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Not Strikethrough

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

Formatted: Font: Not Bold, No underline

c. Service-based accounts, due to their application centric use, are not subject to standard user account management rules.

VI. Compliance and Enforcement

A. The policy applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users who are permitted access.

B. Persons in violation of this policy are subject to a range of sanctions (determined and enforced by institution management), including the loss of computer network access privileges, disciplinary action, dismissal from the institution, and legal action.

C. Some violations may constitute criminal offenses, per Tennessee and other local, and federal laws. The institution will carry out its responsibility to report such violations to the appropriate authorities.

VII. Exceptions

A. Documented exceptions to this policy may be granted by the information security officer for the institution based on limitations to risk and use.

Procedure

Digital Identity and Authentication Management:

Password (and Passphrase) Construction

The effectiveness of passwords to protect access to the institution's information directly depends on strong password construction and handling practices. All users must construct strong passwords for access to all institution networks and systems, using the following criteria (unless the technology does not support these requirements):

For all directions concerning password lengths, password change schedules and the use of passphrases rather than passwords, TBR will follow the NIST standards.

Passwords must be a minimum of 8 characters in length.

Passwords must be composed of a combination of at least three of the following four types of characters:

Upper case alphabetic character;

Formatted: Font: Not Bold, No underline

        - Lower case alphabetic character;
        - Numeric character;
        - Non-alphanumeric character (if the application permits).

        OR

    - Passphrases may be used instead of passwords and must be composed of a minimum of 14 characters. Passphrases do not require the complexity rules mentioned immediately above.

Password Management

- The following requirements apply to **end-user password management**.
    - Storage and Visibility
        - Passwords must not be stored in a manner which allows unauthorized access.
        - Passwords will not be stored in a clear text file.
        - Passwords will not be sent via unencrypted e-mail.
    - Changing Passwords
        - If 14-character minimum pass phrases are used, there is no requirement for routine password expiration/rotation. Otherwise, users with non-privileged accounts must change their passwords every 120 days. Student accounts are exempt from this requirement.
        - Users with privileged accounts (such as those with root or administrator level access) must change their passwords at least every 120 days.
        - Passwords must be changed within one business day if any of the following events occur:
            - Unauthorized password discovery or usage by another person;
            - System compromise (unauthorized access to a system or account);
            - Insecure transmission of a password;
            - Accidental disclosure of a password to an unauthorized person;
            - Status changes for personnel with access to privileged and/or system accounts.
- The following requirements apply to **password files and hashes**.
    - Password files or hashes should not be shared with any entity without formal written consent.
- The following requirements apply to **system accounts**.
    - System Accounts are not required to expire but must meet the password construction requirements above (where supported by the underlying technologies).

Vendor-provided passwords must be changed upon installation using the password construction requirements above (where supported by the underlying technologies).

Compliance and Enforcement

The policy applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users.

Persons in violation of this policy are subject to a range of sanctions determined and enforced by the individual institutions.

Justifications for exceptions to this policy must be documented by the institution and must be approved by the institution's President or his/her designee.

Definitions

Authentication – A process that allows a device or system to verify the unique identity of a person, device or other system that is requesting access to a resource.

Digital identity - Information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device. Also referred to as a user account or user profile.

System account – A special account used for automated processes without user interaction or for device management. These accounts are not assigned to an individual user for login purposes.

Privileged account – An account with elevated access or privileges to a secure system or resource. This type of account is authorized and trusted to perform security relevant functions that an ordinary user account is not authorized to perform. Privileged accounts are assigned to individual users.

~~A.~~

Formatted: Font: Bold

Formatted: No bullets or numbering

Sources

New Guideline approved at President's Meeting August 19, 2014, effective September 26, 2014.

Related Policies

- Information Technology Resources

tbr THE COLLEGE SYSTEM of TENNESSEE

BOARD TRANSMITTAL

MEETING:	Special Called Board Meeting
SUBJECT:	Enterprise Information Systems Updates 1:08:01:00
DATE:	May 14, 2019
PRESENTER:	Danny Gibbs
PRESENTATION REQUIREMENTS:	
ACTION REQUIRED:	Roll Call Vote
STAFF'S RECOMMENDATION:	Approval

BACKGROUND INFORMATION:

This was a guideline that we recommend become a policy. The purpose of this policy is to establish minimum standards of expectations related to maintaining appropriate software versions and upgrades within the institutional infrastructure.

This policy has been reviewed and approved by CIOs at the various institutions, by the Business Affairs Sub-Council and the Presidents.

Attachment(s): Enterprise Information Systems Updates 1:08:01:00

Enterprise Information Systems Updates: 1:08:01:00

Policy Area
Governance, Organization, and General Policies

Purpose
The purpose of this policy is to establish minimum standards of expectations related to maintaining appropriate software versions and upgrades within the institutional infrastructure.

Applies To
TCATs, Community Colleges, System Office, Board Members

Definitions

Third-party products – Software applications that integrate with, or are ancillary to, the ERP system.

ERP quarterly updates – Software updates to the existing ERP system that are developed, tested, approved and released by the SMO each quarter.

Oracle patches and updates – Patches, fixes, and updates for the Oracle Database Server and related components that are released by Oracle on a quarterly basis. These updates may be released off schedule if considered critical.

Critical updates - Widely released software fixes that address specific, serious bugs, problems or defects in a system or application. Sometimes referred to as critical hotfixes or critical patches.

Policy

Enterprise information systems and components used at Tennessee Board of Regents' institutions shall have an established schedule of updates/patches/maintenance to ensure that systems, data, and personally identifiable information (PII) are adequately protected.

I. Scope

A. Enterprise information systems covered by this policy:

1. ERP quarterly updates released by the Ellucian Satellite Maintenance Organization (SMO) shall be installed in their entirety according to the adopted schedule. The institution shall not be more than one version behind the current ERP vendor-certified release and shall make every effort to maintain the latest version release every quarter.
2. Oracle patches and updates shall be installed according to the adopted schedule. The institution shall not be more than one version behind the ERP vendor-

certified Oracle release.

3. Critical updates, patches or hotfixes shall be applied in a timely manner in accordance with institutional needs and requirements, and to minimize (and preferably avoid) unduly exposing the institutions to unnecessary risk.
4. Third-party products supported on the individual campuses must be maintained at a minimum vendor-supported version.

II. Exceptions

A. Exceptions to items 1 and 2 under section I. A. above (Enterprise information systems covered by this policy) must be approved by the President/CEO or his/her designee at the institution and filed with the Chancellor and System CIO, if applicable.

B. Other exceptions to this policy must be approved by the President/CEO or his/her designee and the CIO at the institution.

C. Each exception must be documented in detail and retained for future review.

D. External application and system hosting vendors shall conform to TBR and/or institutional requirements with written exceptions being made as necessary based on the abilities and contractual obligations between the institution and the hosting vendor.

Sources

New Guideline approved at Presidents Meeting, August 19, 2014, effective September 26, 2014. President's Meeting, August 16, 2016. Revised at Presidents Meeting February 21, 2017.

Edited 1/22/2019 by TBR IT Sub Council

THE COLLEGE SYSTEM
of TENNESSEE

BOARD TRANSMITTAL

MEETING:	Special Called Board Meeting
SUBJECT:	IT Acceptable Uses 01:08:05:00
DATE:	May 14, 2019
PRESENTER:	Danny Gibbs
PRESENTATION REQUIREMENTS:	
ACTION REQUIRED:	Roll Call Vote
STAFF'S RECOMMENDATION:	Approval

BACKGROUND INFORMATION:

This was a guideline that we recommend become a policy. Edits include the removal of language associated with universities from the policy, correction of position titles, correction of statute information, and clarification to make the policy more precise in language and to follow updated procedures at the Central Office and TBR Institutions.

This policy has been reviewed and approved by CIOs at the various institutions, by the Business Affairs Sub-Council and the Presidents.

Attachment(s): IT Acceptable Uses 01:08:05:00

IT Acceptable Uses: 01~~G-0541~~:08:05:00

~~Guideline~~Policy Area

General ~~Guidelines~~Policies

Applicable Divisions

TCATs, Community Colleges, ~~**Universities,**~~ System Office, Board Members

Purpose

The objectives of this policy~~guideline~~ include: 1) to articulate the rights and responsibilities of persons using information technology resources owned, leased, or administered by the Tennessee Board of Regents (TBR) and member institutions; 2) to protect the interests of users and the TBR and its member institutions; and 3) to facilitate the efficient operation of TBR and institutional information technology systems.

Definitions

- Information technology resources or IT resources - include computers and computer time, data processing or storage functions, computer systems and services, servers, networks, printers and other input/output and connecting devices, and related computer records, programs, software, and documentation.
- Institutions - shall mean the TBR ~~**Universities,**~~ Community Colleges~~,~~ and Tennessee Colleges of Applied Technology.
- Personal or private for-profit use - shall mean a use of TBR information technology resources which has as a primary objective of financial gain for~~of~~ the user. Activities by a student which are typical of the student job search process (e.g. use of campus e-mail to contact potential employers or posting of one's resume on the i~~I~~nstitution's website, if allowed under i~~I~~nstitutional policies and procedures) are not to be considered personal or private for-profit uses.
- Public record - means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings, or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. T.C.A. § 10-7- 301(6) I.

Formatted: Underline, Strikethrough

Formatted: Strikethrough

Formatted: No underline

Formatted: Strikethrough

Formatted: Font: Not Bold, No underline

~~Guideline~~Policy

I. User Responsibilities

A. The following lists of user responsibilities are intended to be illustrative, and not exhaustive.

1. Access

a. Users shall obtain proper authorization before using TBR or institutional information technology resources.

b. Users shall not use TBR or institutional information technology resources for purposes beyond those for which they are authorized.

c. Users shall not share access ~~privileges~~ credentials.~~(account numbers and passwords) with~~ ~~**persons who are not authorized to use them**~~ ~~**anyone, without modifying passwords**~~.

~~c.~~ ~~**For instance, Auditors require an hexed encrypted document of usernames and passwords from each audited institution. Collecting this file and then immediately forcing a password change would satisfy both the auditors and this policy.**~~

d. Users shall not use TBR or institutional information technology resources in an attempt to access ~~or to actually access computers~~any information technology resources external to the TBR or institution~~system~~ when that access is not authorized by the ~~computer~~system's owner. ~~(no "hacking" allowed).~~

2. Respect for others

a. A user shall not attempt to obstruct usage or deny access to other users.

b. Users shall not transmit or distribute material that would be in violation of existing TBR or institutional policies or guidelines using TBR or institutional information technology resources.

c. Users shall respect the privacy of other users, and specifically shall not read, delete, copy, or modify another user's data, information, files, e-mail or programs

Formatted: Underline, Strikethrough

Formatted: Underline

Formatted: Underline

(collectively, "electronic files") without prior authorization~~the other user's permission~~.

d. Users should note that there should be no expectation of privacy or data retention for~~in~~ electronic files stored on ~~the resident memory of~~ a computer available for general public access~~, and such files are subject to unannounced deletion~~.

e. Users shall not intentionally introduce any program or data intended to disrupt normal operations ~~(e.g. a computer "virus" or "worm")~~ into TBR or institutional information technology resources.

f. Forgery or attempted forgery of e-mail messages is prohibited.

g. Sending or attempts to send unsolicited junk mail or chain letters is prohibited.

h. Flooding or attempts to flood a user's mailbox is prohibited.

3. Respect for State-owned property

a. A user shall not intentionally, recklessly, or negligently misuse, damage or vandalize TBR or institutional information technology resources.

b. A user shall not attempt to modify TBR or institutional information technology resources without authorization.

c. A user shall not circumvent or attempt to circumvent normal resource limits, logon procedures, or security regulations.

d. A user shall not use TBR information technology resources for purposes other than those for which they were intended or authorized.

e. A user shall not use TBR or institutional information technology resources for any private or personal for-profit activity.

f. Except for those not-for-profit business activities which are directly related to an employee's job responsibilities or which are directly related to an organization which is affiliated with the Institution, a user shall not use TBR information technology resources for any not-for-profit business activities, unless authorized by the President ~~**or Director**~~ (or his/her designee).

Formatted: Font: Not Bold, Not Strikethrough

g. Users shall at all times endeavor to use TBR or institutional information technology resources in an efficient and productive manner, and shall specifically avoid excessive game playing, printing excessive copies of documents, files, data, or programs; or attempting to crash or tie-up computer resources.

4. Additional Responsibilities of Employees and Independent Contractors

a. Users who are Employees or~~and~~ Independent Contractors shall not make use of TBR or institutional information technology resources for purposes which do not conform to the ~~purpose,~~ goals~~,~~ and mission of the TBR or institution and to the ~~users~~user's job duties and responsibilities.

b. Users shall not use TBR or institutional information technology resources for solicitation for religious or political causes.

II. Digital/Electronic Signatures and Transactions

A. The Tennessee Board of Regents and its institutions must comply with the Tennessee Uniform Electronic Transactions Act (T.C.A. § 47-10-101 *et seq*.). This Act permits the use of electronic signatures and electronic transactions under certain circumstances.

Formatted: Font: Italic

1. In order to be legally enforceable, an electronic signature must meet the following two criteria.

a. An electronic signature must be attributable (or traceable) to a person who has the intent to sign the record or contract with the use of adequate security and authentication measures that are contained in the method of capturing the electronic transaction (e.g., use of personal identification number or personal log-in identification username and password). (T.C.A. § 47-10- 109) (If Public Key Infrastructure, "PKI" technology ~~("PKI")~~ is to be used in the creation of the digital signature, contact TBR Chief Information Officer prior to implementation.)

b. The recipient of the transaction must be able to print or store the electronic record of the transaction at the time of receipt. (T.C.A. § 47-10- 109)

2. The use of electronic/digital signatures in compliance with state and federal laws is permitted.

III. No ~~No~~ Unlawful Uses Permitted

A. Users shall not engage in unlawful uses of the information technology system resources of the TBR or institution.~~.~~

B. Unlawful activities are ~~violative~~ violations of this policy.~~guideline and may **also** subject~~ ~~p~~Persons engaging in these activities may be subject to civil and/or criminal penalties.

Formatted: Font: Not Bold

Formatted: Font: Not Bold, No underline

C. This list of unlawful activities is illustrative and not intended to be exhaustive.

1. Obscene Materials

~~a.~~ The distribution and display of obscene materials is prohibited by the laws of Tennessee (see T.C.A. § 39-17-902). Obscene materials are defined under Tennessee law (see T.C.A. § 39-17-901(10)).~~ as those materials which:~~

~~1. The average person applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest;~~

Formatted: Indent: Left: 0.79"

~~2. The average person applying contemporary community standards would find that the work depicts or describes, in a patently offensive way, sexual conduct; and~~

~~3.~~a. ~~The work, taken as a whole, lacks serious literary, artistic, political, or scientific value.~~

b. Federal law (18U.S.C.2252) prohibits the distribution across state lines of child pornography.

2. Defamation

a. Defamation is a civil tort which occurs when one, without privilege, publishes a false and defamatory statement which damage the reputation of another.

3. Violation of Copyright

a. Federal law gives the holder of copyright five exclusive rights, including the right to exclude others from reproducing the copyrighted work.

b. Sanctions for violation of copyright can be very substantial. Beyond the threat of legally imposed sanctions, violation of copyright is an unethical appropriation of the fruits of another's labor.

c. Pursuant to the Digital Millennium Copyright Act of 1998, the TBR or institutional designated agent for receipt of complaints of copyright infringement occurring with the use of TBR or institutional information technology resources.

~~c. is the TBR Chief Information Officer or **his/her** designee.~~

d. The TBR or institutional agent shall develop and maintain a guideline regarding receipt and disposition of complaints of copyright infringement.

e. The Institutions are authorized to designate agents to serve their specific campus.~~, however t~~ The TBR and institutional Chief Information Officer shall be promptly informed of ~~as appropriate for~~ complaints received by such Institutional DMCA agents.

4. Gambling

a. Gambling, including that performed with the aid of the Internet, is prohibited under Tennessee state law (see T.C.A. § 39-17-502).

IV. World Wide Web Home Pages

A. The principles of use articulated above in Sections I. and III. are generally applicable to World Wide Web home pages.

1. For example, use of TBR or institutional information technology resources to post a web page for personal or private for-profit use is prohibited under Section I.A.3.e. Illegal content in web pages stored on TBR IT resources is prohibited under Section I.A.2.b. Obscene content is prohibited under Section III.C.1. Incorporation of copyrighted material, without either permission of the copyright holder or under a lawful exemption, is prohibited under Section III.C.3.

2. In addition to the principles of use outlined in Sections I. and III., users may not incorporate into web pages or other electronic documents the trademarks or logos of others without express, written permission.

3. Persons who are not employees of an Institution may not make use of Institutional trademarks or logos without express, written permission.
4. Institutions are authorized to develop policies and regulations regarding use of Institutional trademarks on the Institution's website by employees.
5. The Institution Presidents ~~and Directors~~ are authorized to designate persons (e.g. campus web master) who may approve a proposed use of the Institution's trademarks and logos by employees on Institutional web pages.

V. Advertising

A. Use of TBR or institutional information technology resources to promote or advertise activities or entities which are not related to the Institution is prohibited, unless such use is consistent with the mission of the Institution and results in substantial benefit to the Institution.

B. The President ~~or Director~~ of each TBR Institution is authorized to determine whether a given use is consistent with the mission of the Institution and results in substantial benefit to the Institution, consistent with other TBR p~~P~~olicies/guidelines.

~~B. (in particular, TBR Policy 1:03:02:50).~~

C. Sale of advertising in web-based versions of Institution-affiliated student publications is specifically permitted.

~~C.~~

Formatted: Indent: Left: 0.52", No bullets or numbering

VI. TBR Monitoring and Inspection of Electronic Records

A. Electronic records sent, received, or stored on computers owned, leased, or administered by the TBR is the property of the Tennessee Board of Regents.

B. As the property of the TBR, the content of such records, including electronic mail, is subject to inspection by TBR personnel.

C. While the TBR does not routinely do so, the TBR ~~is able and~~ reserves the right to monitor and/or log all network activity of users without notice, including all email and Internet communications.

D. Users should have no reasonable expectation of privacy in the use of these resources.

VII. Disclosure of Electronic Records

A. Pursuant to T.C.A. § 10-7-101 *et sq*., and subject to exemptions contained therein, electronic files (including email correspondence) may be subject to public inspection upon request by a citizen of the State of Tennessee, if they are:

Formatted: Font: Italic

1. Generated or received by TBR or institutional employees, and
2. Either owned or controlled by the State, or
3. Maintained using TBR or institutional IT resources.

B. TBR or institutional personnel receiving such a request for public inspection should refer the request to the President ~~or Director~~ of their Institution (or to the President's ~~or Director's~~ designee).

C. Institutions may charge reasonable fees for making copies of such records, pursuant to T.C.A. § 10-7-506.

D. While disclosure under T.C.A. § 10-7-101 *et sq*. applies to employees, disclosure of the electronic records of all users which are maintained using TBR or institutional IT resources may be made pursuant to a valid subpoena or court order, when otherwise required by federal, state or local law, or when authorized by the President ~~or Director~~ of the Institution.

Formatted: Font: Italic

VIII. Retention of Electronic Records

A. Electronic records needed to support Institutional functions must be retained, managed, and made accessible in record-keeping or filing systems in accordance with established records disposition authorizations approved by the Public Records Commission and in accordance with TBR Guideline G-070, "Disposal of Records".

B. Each employee of the TBR, with the assistance of his or her supervisor as needed, is responsible for ascertaining the disposition requirements for those electronic records in his or her custody.

C. The system administrator is not responsible for meeting the record retention requirements established under T.C.A. § 10-7-101 et sq., and the TBR, as owner of electronic records stored on TBR computers, reserves the right to periodically purge electronic records, including email messages.

D. Users who are either required to retain an electronic record, or who otherwise wish to maintain an electronic record should either:

1. Print and store a paper copy of the record in the relevant subject matter file; or
2. Electronically store the record on a storage medium or in an electronic storage location not subject to unannounced deletion.

IX. Violation of this Policy~~Guideline~~

A. Reporting Allegation of Violations

1. Persons who have reason to suspect a violation of this policy~~guideline~~, or who have direct knowledge of behavior in violation of this policy~~guideline~~ should report that allegation of violation to the Institution President ~~**or Director**~~ or ~~**his/her**~~ designee.

B. Disciplinary Procedures

1. Allegations of violation of this policy~~guideline~~ shall be referred by the President or his/her designee ~~the designee of the President (typically, the senior IT officer)~~ ~~**or of the Director**~~ to the appropriate person(s) for disciplinary action.
2. If a student, the policy~~guideline~~ violation will be referred to the judicial officer of the institution under TBR Policy 3:02:00:01.
3. If an employee, the policy~~guideline~~ violation will be referred to the immediate supervisor.
4. If there is a policy~~guideline~~ violation, which the designee believes rises to the level of a serious violation of this or any other TBR policy~~/guideline~~; the designee is authorized to temporarily revoke access privileges. In those cases, the revocation of access must be reviewed by the appropriate disciplinary authority for review and final determination of access privileges. In such cases the authorization of the designee carries with it the authorization to make subjective judgments, such as whether material or statements violate TBR Policy/Guideline.

C. Sanctions

1. Persons violating this policy~~guideline~~ are subject to revocation or suspension of access privileges to TBR or institutional IT resources.
2. Additionally other penalties, as outlined in TBR Policy 3:02:00:01 may be imposed upon student users.
3. Sanctions for violation of this ~~guideline~~ policy by employees may extend to termination of employment. Violations of law may be referred for criminal or civil action.

D. Appeals

1. Sanctions imposed upon students at a TBR ~~University or Community College~~institution and imposed at the discretion of the President or his/her designee ~~senior IT officer (or other designee of the President)~~ may be appealed ~~to the Chief Student Affairs Officer.~~through the appropriate process per TBR and/or institutional policy.
2. Other sanctions may be appealed under established Institution procedure.

Formatted: Font: Not Bold, Not Strikethrough

Formatted: Font: Not Bold, Not Strikethrough

Sources

NEW Guideline approved at Presidents Meeting February 21, 2017.

Related Policies

- Information Technology Resources

tbr THE COLLEGE SYSTEM *of* TENNESSEE

Special Called Meeting of the Board
May 14, 2019

SUBJECT: Policy Revision: 2:01:00:04
Awarding of Credits Earned Through Extra-Institutional
Learning to Community Colleges

PRESENTER: Randolph Schulte, Ed.D.
Vice Chancellor for Academic Affairs

ACTION REQUIRED: Roll Call Vote

Summary:

The purpose of this policy is to authorize each community college governed by the Tennessee Board of Regents to develop procedures for the recognition of equivalent extra-institutional learning processes that include the awarding of credit or advanced placement. These processes are also referred to as Prior Learning Assessment (PLA). This policy reaffirms the institutions' compliance with SACSCOC updated to include the reference (10:8) to the 2018 Principles of Accreditation. This policy also reaffirms compliance of institutional PLA policies with the *Recommended Standards in Prior Learning Assessment (PLA) Policy and Practice of Tennessee Public Colleges and Universities*, which were developed statewide under the auspices of THEC in 2012.

This policy has been revised to conform with the new TBR policy format. There are no substantive changes in this policy. This policy has been reviewed and approved by the Academic Affairs Subcouncil, the Student Affairs Subcouncil, the Faculty Subcouncil and the Presidents Council.

Attachments: TBR Policy 2:01:00:04 Awarding of Credits Earned Through Extra-Institutional Learning to Community Colleges

Policy Category: 2 – Academic Policies

Policy Number: 2:01:00:04

Policy Name: Awarding of Credits Earned Through Extra-Institutional Learning to Community Colleges

Applies to: Community Colleges

Purpose

The purpose of this policy is to authorize each community college governed by the Tennessee Board of Regents to develop procedures for the recognition of equivalent extra-institutional learning processes that include the awarding of credit or advanced placement.

Policy

I. Extra-Institutional or Life-long Learning

A. The process for awarding of credits through "Extra-Institutional or Life-long Learning" also referred to as Prior Learning Assessment (PLA) by the community colleges must be in compliance with the Commission on Colleges of the Southern Association of Colleges and Schools' Principles of Accreditation (reference 10:8) and the Commission's Position Statement on the "Transfer of Academic Credit."

B. The institutional process for awarding credits through Prior Learning Assessment (PLA) by TBR community colleges must be in compliance with the *Recommended Standards in Prior Learning Assessment (PLA) Policy and Practice of Tennessee Public Colleges and Universities (August 7, 2012)* (Exhibit 1).

1. These Standards ensure that TBR colleges will utilize best practices and provide services to students that are consistent among institutions.

2. The Standards ensure transferability of PLA credit, include identification of types of PLA credits available, instruct campuses on the transcription of PLA credit, and establish common standards for portfolio review.

C. When awarding credit under this provision, the institution should use a recognized guide or institutional procedure for awarding the credit for extra-institutional or life-long learning. The recognized guides or institutional procedures may include but are not limited to:

1. American Council on Education (ACE) National Guide to Educational Credit for Training Programs.

2. Guide to Credit by Examination.

3. College ~~Entrance Examination~~ Board Advanced Placement Program. (~~CEEB/~~AP)

4. College Level Examination Program (CLEP)

5. Defense Subject Standardized Test (DSST) formerly DANTES.

6. Credit by Departmental Examination.

7. Subject matter experts who are not members of the institution's faculty but who evaluate extra-institutional learning at the institution's request.

8. Individual portfolios using the Council for Adult and Experiential Learning (CAEL) or other standardized guidelines authorized, in advance, by permission of the institution.

D. When awarding credit to students who are veterans or military service members, the institution will reference the Joint Services Transcript (JST), DD-214 and/or transcripts from the Army/American Council on Education Registry Transcript System (AARTS), Community College of Air Force (CCAF), and Coast Guard Institute (CGI). The institution will use the American Council of Education (ACE) for awarding credit for military experience, educations, and/or training obtained during military experience. The recognized procedures include:

1. If military experience, education, and/or training are equivalent to a course that fulfills a general education or degree program requirement, the course credit will count towards graduation. Otherwise, appropriate course credit will be granted for elective credit.

2. Should credit not be captured through ACE recommendations, TBR institutions will offer veterans and service members an opportunity for prior learning assessment via another recognized mechanism (refer to Section C, above).

3. Each TBR institution will provide veteran and military service members relevant information on awarding college credit for military education, experience, and/or training.

4. Each TBR institution will maintain a set of institutional polices on the awarding of academic credit for military experience within their undergraduate catalog. The policies will include a description of the procedure for removing excessive hours applied to transcripts, which may affect student eligibility for financial aid.

Sources

T.C.A. § 49-8-203

History

March 2006 TBR Board Meeting; Revised September 20, 2013. Revisions approved by Board September 15, 2016.

Exhibits

Recommended Standards in Prior Learning Assessment (PLA) Policy and Practice of Tennessee Public Colleges and Universities (August 7, 2012)

tbr THE COLLEGE SYSTEM
of TENNESSEE

Special Called Meeting of the Board
May 14, 2019

SUBJECT:	Policy Revision 2:02:00:01 ROTC (Reserve Officer Training Corps) Programs
PRESENTER:	Randy Schulte, Ed.D. Vice Chancellor, Academic Affairs
ACTION REQUIRED:	Roll Call Vote

Summary:

Policy 2:02:00:01 ROTC Programs has been reformatted according to new structural convention, and the Purpose section has been revised. No substantive changes have been made.

The proposed policy revision has been reviewed and approved by General Counsel, Academic Affairs Subcouncil, Faculty Subcouncil and the Presidents Council.

Attachments:

Policy 2:02:00:01 ROTC Programs

~~ROTC Programs: 2:02:00:01~~

2 – Academic Policies

2:02:00:01

~~Policy Area~~

~~Academic Policies~~

~~Applicable Divisions~~

~~Community Colleges, Universities~~

Purpose

~~The purpose of this policy is the establishment of policy regarding ROTC Programs at institutions governed by the Tennessee Board of Regents.~~

Reserve Officer Training Corps (ROTC) prepares students to become officers in the United States military. The Tennessee Board of Regents establishes this policy in support of this opportunity for leadership training and preparation for service to country as part of a student's post-secondary education program of study.

Applies to: Community Colleges

Policy

Community colleges may enter into cooperative agreements with other higher education institutions to offer ROTC instruction to their students.

Procedures

A. Cooperative ROTC programs shall be designed by the participating institutions to best serve the interests of students wishing to enroll in ROTC.

B. A copy of the final agreement must be forwarded to the Office of the Vice Chancellor for Academic Affairs at the Tennessee Board of Regents for approval.

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Bold, Font color: Custom Color(RGB(52,64,81))

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Bold, Font color: Custom Color(RGB(52,64,81))

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: (Default) Times New Roman, 12 pt

~~I. ROTC Programs~~

Formatted: Font: (Default) Times New Roman

~~A. The universities and community colleges under the governance of the State Board of Regents may enter into cooperative agreements with other institutions of higher education to offer ROTC instruction to their students.~~

~~B. The details of the cooperative programs shall be worked out between the individual institutions so that the interests of students wishing to enroll in ROTC are best served.~~

~~C. When the final arrangements have been agreed upon by the institutions, a copy of the agreement shall be forwarded to the office of the State Board of Regents.~~

Formatted: Font: (Default) Times New Roman, 12 pt

Sources

TBR Meeting, June 22, 1973

Formatted: Font: (Default) Times New Roman

Related Policies

Exhibits

Approvals

Formatted: Font: (Default) Times New Roman, 12 pt

tbr THE COLLEGE SYSTEM of TENNESSEE

Special Called Meeting of the Board
May 14, 2019

SUBJECT: Policy: 5:02:05:00
Employment of Graduate Assistants

PRESENTER: Randolph Schulte, Ed.D.
Vice Chancellor for Academic Affairs

ACTION REQUIRED: Roll Call Vote

Summary:

The Academic Affairs staff and the Human Resources Advisory Committee reviewed TBR Policy 5:02:05:00 Employment of Graduate Assistants. As TBR institutions do not enroll graduate degree-seeking students and as the employment of graduate students from other institutions is governed under normal employment policies, the dissolution of this policy is recommended. The Academic Affairs Subcouncil, Faculty Subcouncil and Presidents Council each concurred with this recommendation for dissolution.

Attachments
Policy: 5:02:05:00 Employment of Graduate Assistants

RECOMMENDED DISSOLUTION

Formatted: Font: 12 pt, Font color: Background 2

Employment of Graduate Assistants: 5:02:05:00

Policy Area

Personnel Policies

Applicable Divisions

Community Colleges,

Purpose

The purpose of this policy is to establish the criteria and process regarding employment of graduate assistants at institutions governed by the Tennessee Board of Regents.

Policy

I. Introduction

A. Institutions of TBR the College System of Tennessee may employ graduate assistants according to the following guidelines and descriptions.

II. Workload

A. Full-time graduate assistants will work:

1. Six (6) contact hours per week in classroom or laboratory instruction;
2. Eight (8) contact hours per week in laboratory supervision;
3. Twenty (20) clock hours per week in supervised activities in the department of their employment; or
4. A combination of the above.

III. Terms of Employment

A. The specific terms of the employment may be for an academic year, quarter, semester, fiscal year, or based upon a percentage of full-time assistantship.

IV. Salary Schedule

A. Each institution that employs graduate assistants shall have a salary schedule which takes into account the particular needs and priorities of the institution.

V. Eligibility

RECOMMENDED DISSOLUTION

Formatted: Font: 12 pt, Font color: Background 2

A. A student must be accepted and/or enrolled in the graduate program to be eligible for appointment as a graduate assistant.

B. On campuses that include a public school, private or parochial school, licensed day care center, other child care facility, public park, playground, recreation center or public athletic field available for use by the general public or campuses that are within one thousand feet (1000') of a public school, playground, recreation center or public athletic field available for use by the general public, no student who is registered as a sex offender pursuant to the Tennessee Sexual Offender and Violent Sexual Offender Registration, Verification, and Tracking Act of 2004 is eligible to be an institutional employee who is compensated with taxable wages.

1. On such campuses, a student who is a registered sex offender is eligible for an appointment as a graduate assistant only if he or she is not receiving any taxable wages or taxable stipends as compensation, and the monetary compensation for the student is limited to awards of non-taxable scholarship or grant funds.

VI. Payment

A. Salary payments should be made on a monthly basis or at a regularly scheduled time for salary payments to full-time personnel of the institution.

Sources

TBR Meetings: August 17, 1973; December 12, 1980; December 2, 1988; June 29, 1990; September 21, 1990: March 28, 2008. Ministerial revision June 23, 2015.